What is claimed is:

Claims:

1. A method for effecting secure transactions over a computer network in a manner designed to foil identity theft perpetrated from an untrusted computer, comprising:

connecting a client computer to the network wherein the client computer provides a user interface to interact with a user;

connecting a server computer to the network;

connecting a portable secure computing device to the network;

operating the secure computing device to communicate a list of available services to the client computer;

responsive to receiving the list of available services using the user interface to display the list of available services to a user;

responsive to a selection of one available service by the user, establishing a secure connection from the secure computing device to the server;

securely communicating private information from the secure computing device to the server over the secure connection.

2. The method of Claim 1 further comprising:

authenticating a user based on the private information; and

in response to successful authentication of the user, conducting a transaction between the client computer and the server computer.

3. The method of Claim 1 further comprising:

transmitting from the secure computing device to the server computer user identifying information.

4. The method of Claim 3 wherein the user identifying information includes a secret personal identification number (sPIN).

5. The method of Claim 4 further comprising:

responsive to receiving the user identifying information, operating the server computer to establish an association among the user, the client and the secure computing device.

6. The method of Claim 4 wherein the secure computing device has a personal identification number (PIN) wherein the sPIN and the PIN are unrelated.

7. The method of Claim 4 wherein the server computer uses the sPIN for only one session.

8. The method of Claim 1 wherein the portable secure computing device is a smart card.

9. A method for secure transactions over a computer network in a manner designed to foil identity theft perpetrated from an untrusted computer, comprising:

connecting a client computer to the network wherein the client computer provides a user interface to interact with a user;

connecting a server computer to the network;

connecting a secure computing device to the network;

establishing a secure connection from the secure computing device to the server;

securely communicating private information from the secure computing device to the server over the secure connection;

authenticating a user using the private information; and

in response to successfully authenticating the user, conducting a transaction between the client and the server.

10. The method of Claim 9 wherein the step of securely communicating private information comprises pushing the private information from the secure computing device to the server computer.

11. The method of Claim 10 further comprising:

in response to successfully authenticating a user, operating the client to transmit an indication to the server that the secure computing device will send information necessary for a transaction;

operating the server to wait for the information from the secure computing device;

operating the client to select the information necessary for the transaction; and

in response to selecting the information necessary for the transaction, operating the secure computing device to transmit the selected information securely to the server.

12. The method of Claim 9 wherein the step of securely communicating private information comprises operating the server computer to pull the private information from the secure computing device.

13. The method of Claim 9 further comprising:

in response to successfully authenticating a user, operating the server to transmit a request to the secure computing device to provide information necessary to complete a transaction;

in response to a request from the server for information necessary to complete a transaction, operating the secure computing device to notify the client that the server has made the request for information necessary to complete a transaction;

in response to notification from the secure computing device that the server is requesting the information necessary to complete a transaction, operating the client to obtain a user's approval or denial of the request; and

in response to a user's approval, transmitting the requested information from the secure computing device to the server in a secure manner.

14. A system for effecting secure transactions over a computer network in a manner designed to foil identity theft through keystroke logging, comprising:

a server computer connected to a computer network and operable to provide some form of online transactions;

a client computer connected to the computer network and operable to interface with a user;

a secure computing device connected to the computer network and capable of establishing a secure connection with the server computer and the client computer;

wherein the secure computing device has logic operable to store private user information; and

wherein the secure computing device has logic, in response to the initiation of a transaction between a user operating the client computer and the server computer, operable to securely transmit the private user information to the server computer in a manner such that only the server can interpret the private user information.

15. The system for effecting secure transactions over a computer network of Claim 14:

wherein the secure computing device has logic to transmit a map to the server computer, the map having the elements clientIP, cardIP, login credentials, and secret personal identification number (sPIN);

wherein the server computer has logic to request a user to enter the sPIN and logic to verify that the entered sPIN matches the sPIN in the map.

16. The system for effecting secure transactions over a computer network of Claim 15:

wherein the server computer has logic to destroy the map if the sPIN entered by the user does not match the sPIN of the map.

17. The system for effecting secure transactions over a computer network of Claim 14:

wherein the portable secure computing device transmits the private user information upon a request by the user.

18. The system for effecting secure transactions over a computer network of Claim 14:

wherein the portable secure computing device transmits the private user information upon a request by the server computer.

19. The system for effecting secure transactions over a computer network of Claim 18:

wherein the portable secure computing device transmits the private user information to the server computer only upon permission granted by the user.

20. The system for effecting secure transactions over a computer network of Claim 19:

wherein the server computer destroys the map in response to invalid sPIN, denial of permission from the user, and transaction completion.